SBC service into MiVoice 5000 Server, EX Controller and Mitel 5000 Compact

04/2025
AMT/PTD/PBX/0138/3/0/EN
IMPLEMENTATION MANUAL

Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®).

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries.

Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

CONTENTS

1 ABOUT THIS DOCUMENT

1.1 PURPOSE OF THIS DOCUMENT

This document describes how to implement the SBC service in a MiVoice 5000 environment. The use of the SBC is suitable for the following Mitel systems:

- MiVoice 5000 Server
- Mitel 5000 Compact
- Mitel EX Controller

1.2 ABBREVIATIONS

Mitel 5000 Gateways	This term refers to all XS, XL and XD iPBXs.
MiVoice 5000 Server	Telephony switching system running on a Linux
XS, XL, XD	MiVoice 5000 series physical gateways.
XS	This term includes XS, XS12 and XS6 systems
MiVoice 5000 Manager	Systems management centre
CAC	Call Admission Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	Demilitarised zone
FTP	File Transfer Protocol.
IP	Internet Protocol
ITF	Interface
LAN	Local Area Network
NAT	Network Address Translation
iPBX	IP Private Branch eXchange
PBX	Private Branch eXchange
PKI	Public Key Infrastructure
MMC	Man Machine Command, iPBX command.
RTP	Real Time Protocol
SBC	Server Base Computing
SIP	Session Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

1.3 REFERENCE DOCUMENTS

To better understand this document, refer to the following documents in Mitel's Document Center:

- MiVoice 5000 Server – Implementing Manual
- MiVoice 5000 Server – Operating Manual
- MiVoice 5000 Manager – Installation and Configuration
- MiVoice 5000 Manager – User Guide
- CloudLink – Deployment Guide with MiVoice 5000
- Mitel 5000 Compact – Quick

1.4 REMINDER CONCERNING THE LAW ON INFORMATION TECHNOLOGY

The user is reminded that the use of PBXs in the workplace must comply with the recommendations of the IT law in force.

The user's attention is also drawn to any clauses applicable in laws relating to the confidentiality of calls transmitted by means of telecommunications.

2 GENERAL INFORMATION

2.1 INTRODUCTION

The SBC service is integrated to the MiVoice 5000 Server, the Mitel EX Controller and the Mitel 5000 Compact.

The MiVoice 5000 uses the SBC service in two situations:

- For SBC trunks,
- To support subscribers in OTT mode

The service can be implemented from Web Admin and consists in configuring the different IP addresses on the public and private side for address translations in the architecture in question. For an EX Controller or a Mitel 5000 Compact, the network interfaces must be in different subnets.

The integrated service also contains some security upgrades using some filters on the IP address lists to protect themselves from DDoS and DoS type attacks.

The SBC service also include video sessions.

2.2 REMINDER ON NAT RELATED PROBLEMS

NAT network devices (routers, firewall, etc.) translate addresses, for security reasons and/or due to lack of public IPv4 addresses. The addresses are translated on the IP header, but not always on encapsulated IP addresses (on the application header).

The SIP conveys private RTP negotiation IP addresses/ports. The (RTP) audio flow may be locked by the client's NAT network devices due to unknown (untranslated) addresses.

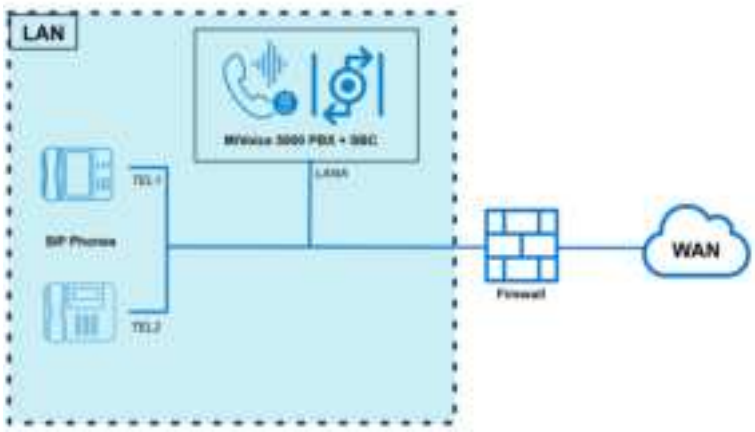
The solution proposed via the SBC service allows you to offer telephone services to an SIP operator, by passing through the network devices of the client managing the NAT, and if necessary, compensating for the NAT for the network devices that do not fully manage the NAT for encapsulated IP addresses.

2.3 SBC SERVICE ARCHITECTURES

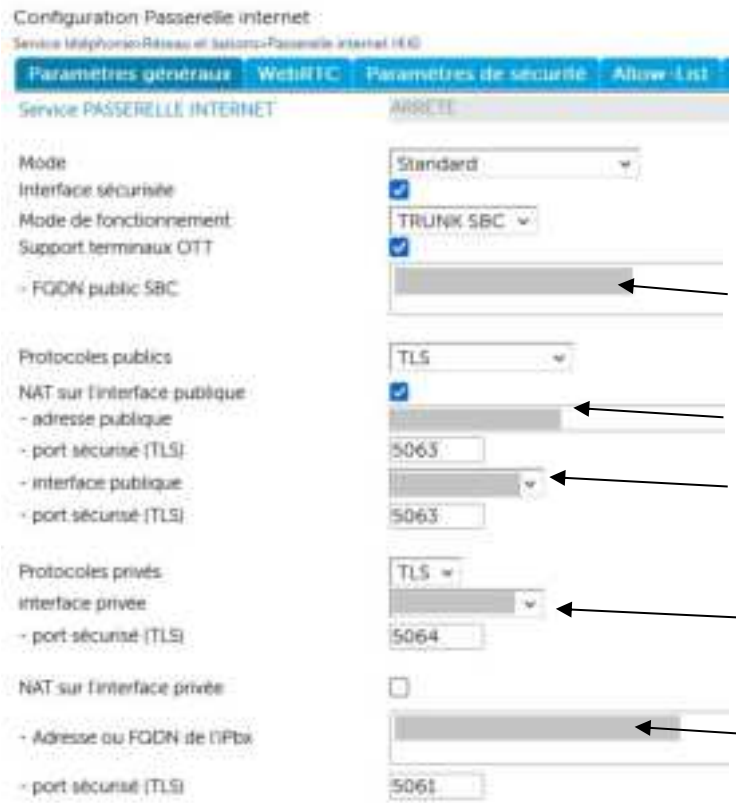
The SCB service can work under different architecture cases. This paragraph only describes the most frequent cases in a MiVoice 5000 environment.

2.3.1 SBC AND PBX IN THE SAME MACHINE

For small installations, installers usually use this architecture



Depending on the configuration (using NAT or OTT mode), the installer may configure the menu **Telephony service>Network and links>Internet gateway** – **General settings** tab as followed :



Public FQDN of the SBC (depending on the configuration)

Public IP@ of the SBC WAN

IP@ LANA

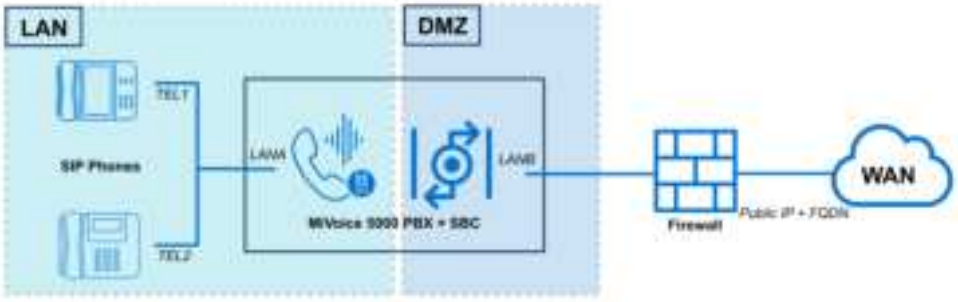
IP@ LANA

IP@ LANA

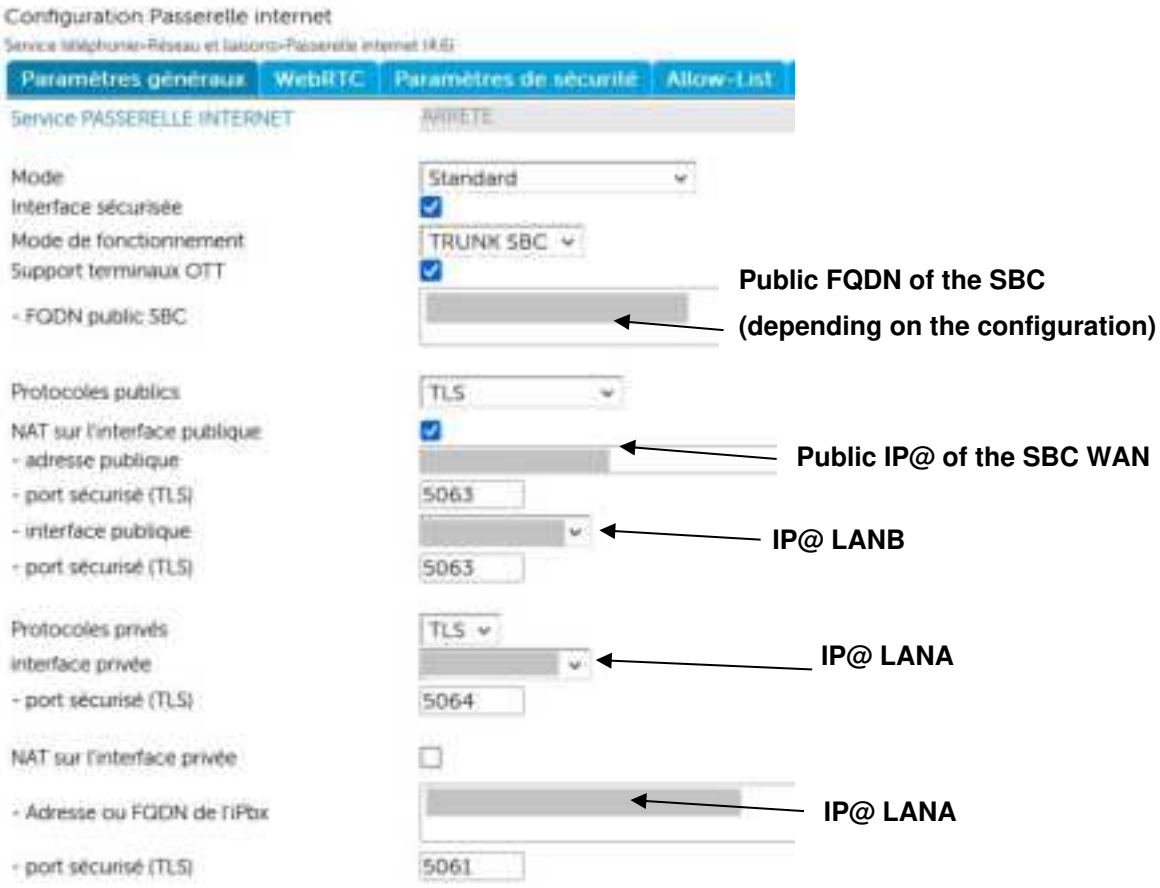
2.3.2 SBC AND PBX IN THE SAME MACHINE, LAN/DMZ SEPARATED

This architecture is mostly used when the needed configuration requires a second IP address for the SBC trunk

Reminder : If using an EX Controller or a Mitel 5000 Compact with two network interfaces, the network cards ust be on separate subnets.

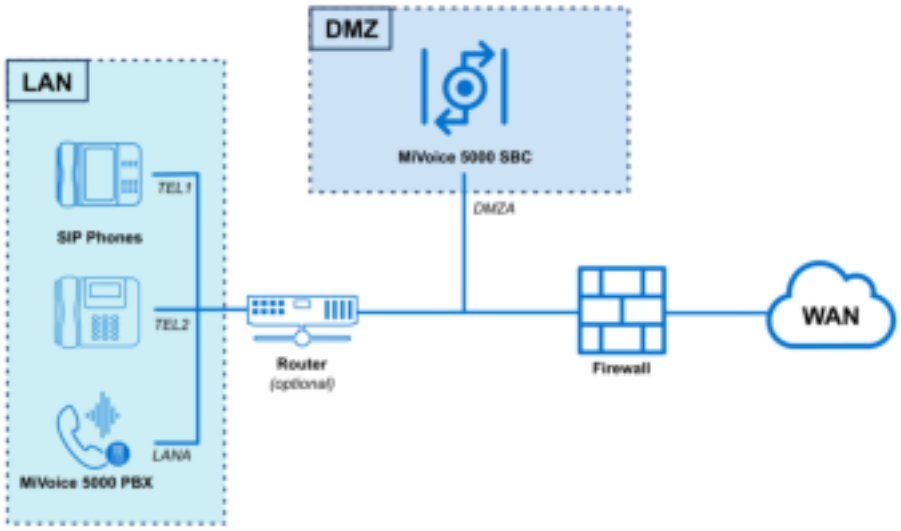


Depending on the configuration (using NAT or OTT mode), the installer may configure the menu **Telephony service>Network and links>Internet gateway** – **General settings** tab as followed:



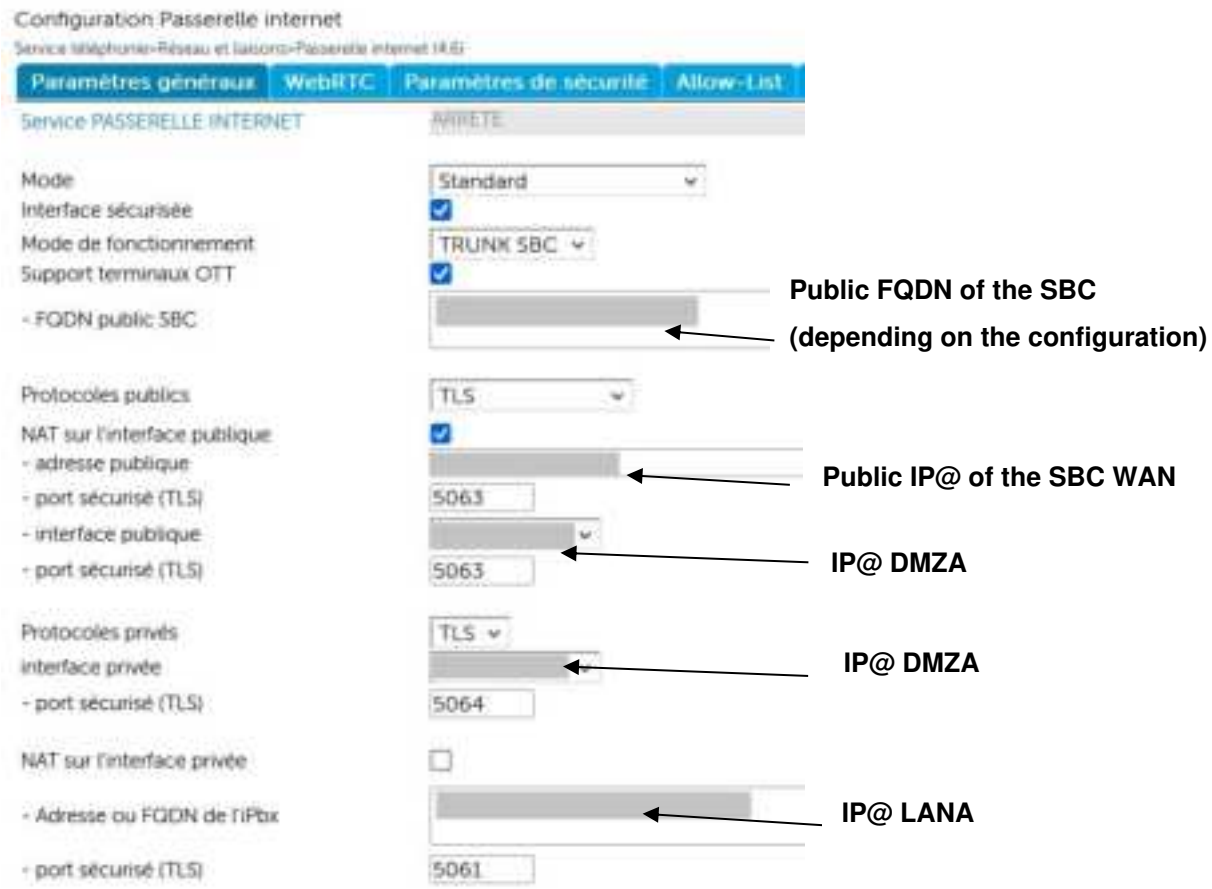
2.3.3 SBC AND PBX IN DIFFERENT MACHINES

This architecture with separated SBC and PBX illustrates a secure installation with an SBC in DMZ and a PBX in LAN.



Note: If there is a firewall between the DMZ and the LAN, the RTP ranges and the subnets of the devices must have access to the DMZ.

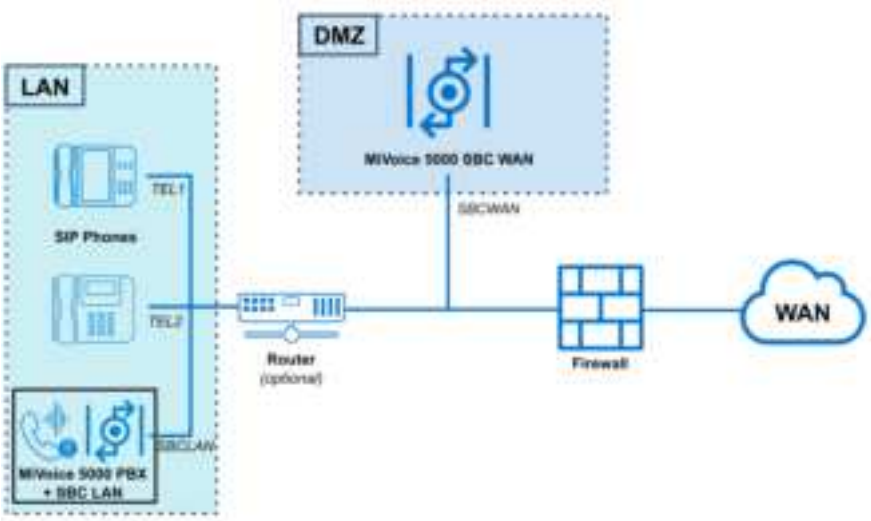
Depending on the configuration (using NAT or OTT mode), the installer may configure the menu **Telephony service>Network and links>Internet gateway** – **General settings** tab as followed:



2.3.4 DAISY CHAIN SBC WITH PBX IN THE SAME MACHINE

In a Daisy Chain configuration, the architecture includes 2 distinct SBC:

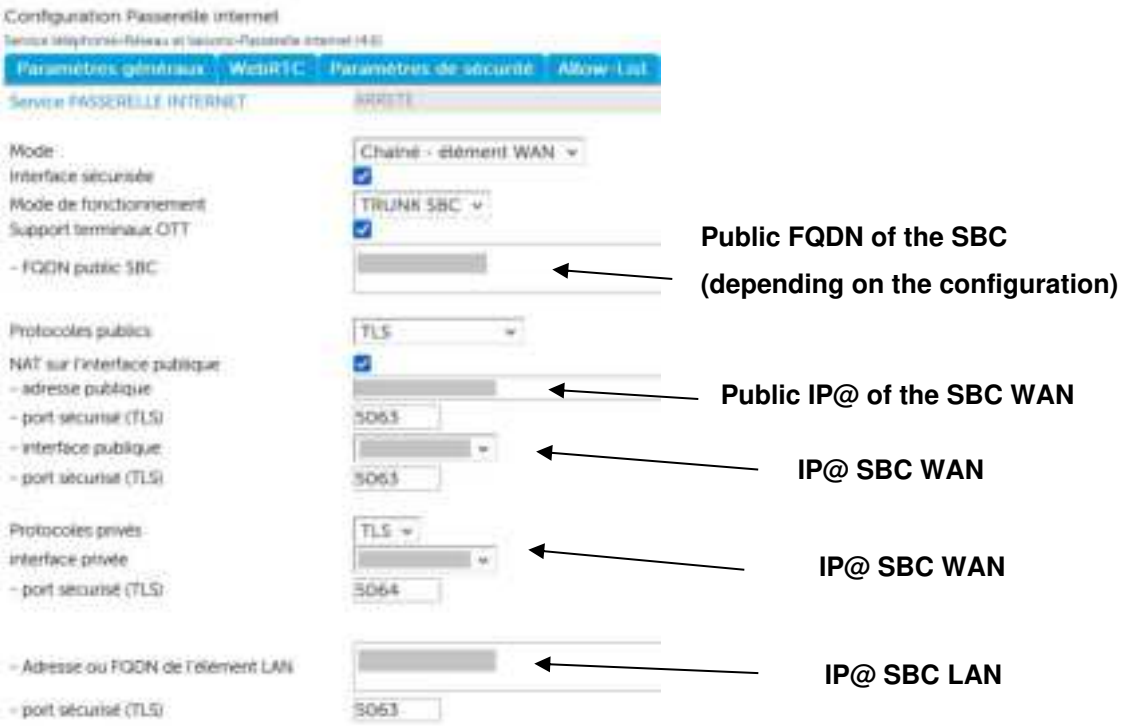
- The first SBC is in DMZ. In the configurations requiring an SBC, connections (SIP TLS, voice, etc.) goes through this SBC. The SBC in DMZ communicates only with the SBC in LAN, in this case.
- The second SBC is in LAN. In this specific configuration, both LAN PBX and SBC are in the same machine.



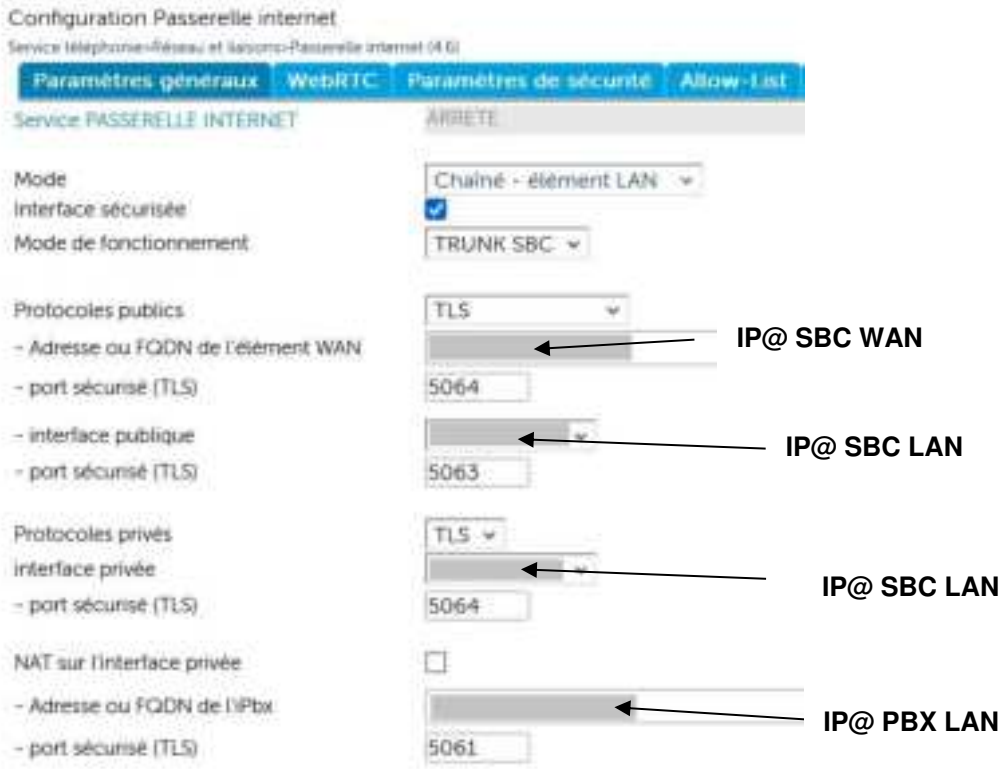
Note: If there is a firewall between the DMZ and the LAN, the RTP ranges must have access to the DMZ.

Depending on the configuration (using NAT or OTT mode), the installer may configure the menu **Telephony service>Network and links>Internet gateway** – **General settings** tab as followed:

- On the SBC of the MiVoice 5000 in DMZ (SBC WAN in the figure)

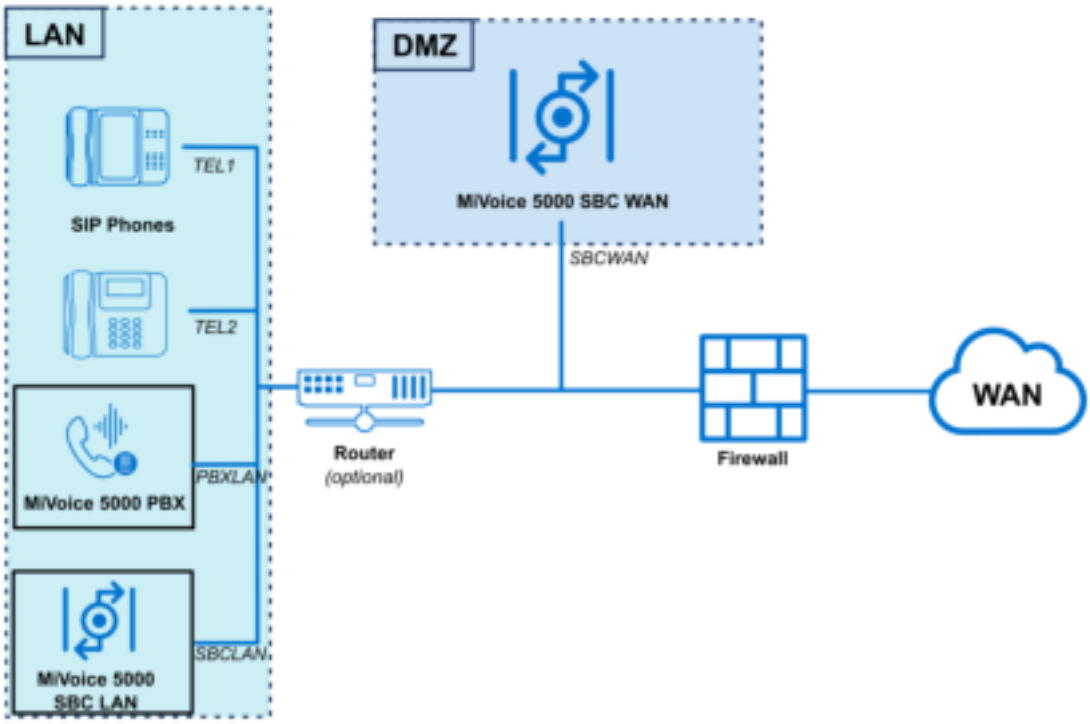


- On the SBC of the MiVoice 5000 in LAN (SBC LAN in the figure)



2.3.5 DAISY CHAIN SBC WITH PBX IN DIFFERENT MACHINES

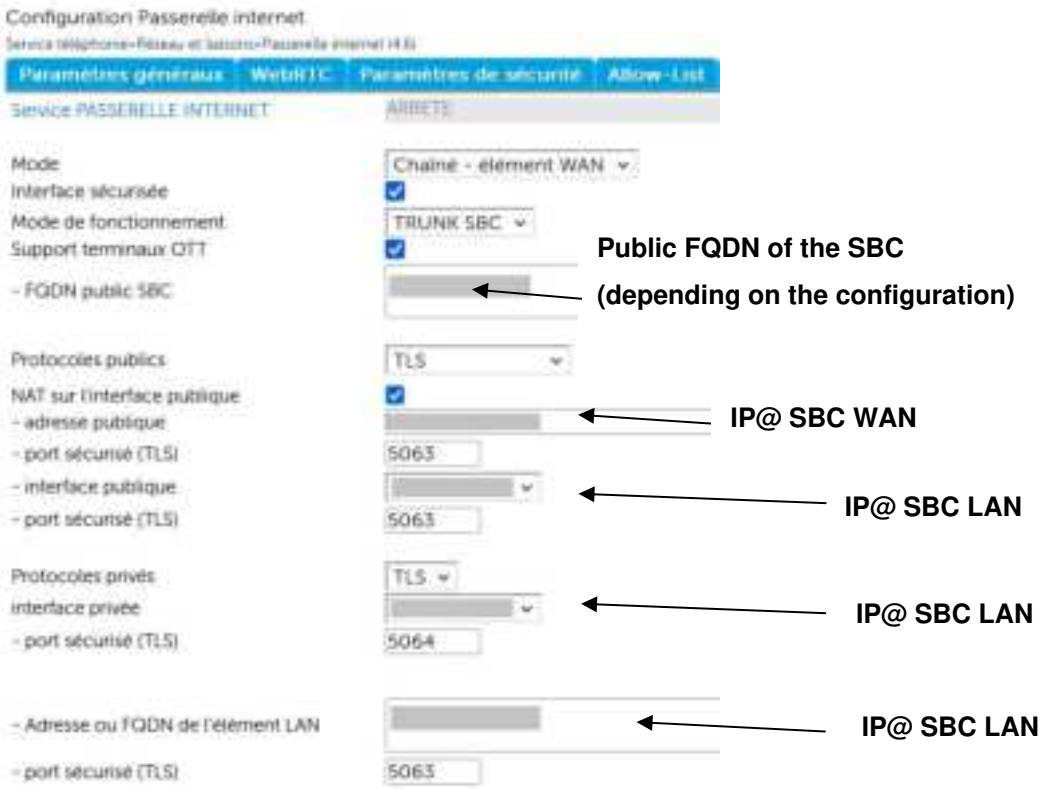
This architecture is a variant of the previous one. Here, the LAN PBX and the SBC are on different machines.



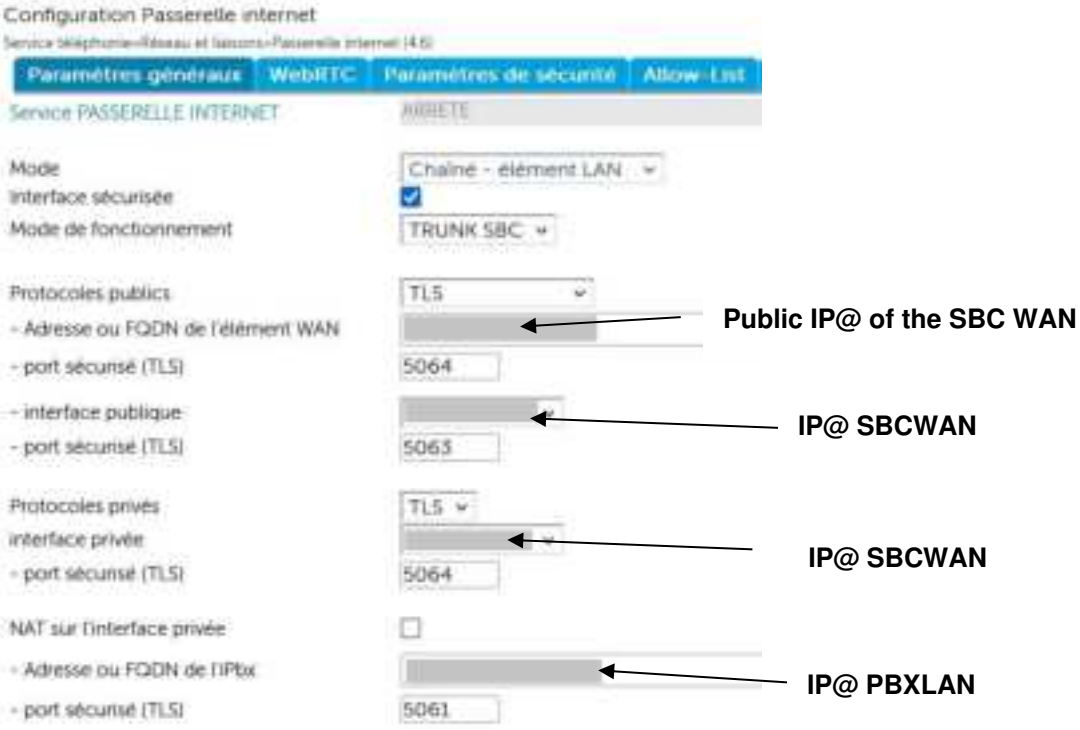
Note: If there is a firewall between the DMZ and the LAN, the RTP ranges must have access to the DMZ.

Depending on the configuration (using NAT or OTT mode), the installer may configure the menu **Telephony service>Network and links>Internet gateway** – **General settings** tab as followed:

- On the SBC of the MiVoice 5000 in DMZ (SBC WAN in the figure)



- On the SBC of the MiVoice 5000 in LAN (SBC LAN in the figure)



2.4 STARTING THE SBC SERVICE

The Menu Telephony **service>System>Configuration>Services (2.3.1)** can Start / Stop / Restart the SBC service.

2.5 LICENSE

To use SBC trunks, the SBC service requires à ciphering license only if the wanted configuration includes a TLS trunk with STRP. Otherwise, the SBC service is available without any specific license.

2.6 SECURITY LEVEL

2.6.1 PRINCIPLE

The SBC provides the following services on MiVoice 5000 Server only and for trunk calls:

- NAT signalling/media
- Audio/video transport
- Defence against SIP DoS (flooding or Malicious call) and SIP DDoS attacks.
- The Qualiyt of Service (QoS)

The security service can be activated to protect the system against certain Flooding-type DoS or DDos attacks:

- **DoS**, using a Allow-List (trusted IP addresses) and a Deny-List
- **DDoS**, using a filter.

As the SBC service is dedicated to the SIP trunk, the protection against **Force Brute** attacks is not implemented.

Regardless of the activation of security, the SBC is protected against Malicious Call-type DoS attacks.

The Allow-List (**Allow-List tab)** comprises some trusted IP addresses declared by the installer. However, these IP addresses remain subject to checks against Malicious Call attacks.

The Deny-List (**Deny-List DoS** tab) is not configurable and is filled in dynamically by the IP addresses considered as attacking.

These IP addresses are contained in the security criteria defined for SIP DoS (flooding or Malicious call) attacks.

The IP addresses are entered for a configurable period (1 hour by default). The list can also be cleaned by the installer (see next paragraphs).

2.6.2 CHOOSING THE SECURITY LEVEL

Menu **NETWORK AND LINKS> Internet Gateway – Security parameters** tab

The first parameter is used to configure the implemented security parameter.

The options proposed by the dropdown list are:

- None
- Self protection
- Allow-list only

Description of the different options:

None:

The **Allow-List** tab is not accessible.

Even if security is disabled, Malicious Call check is systematically made; the **DoS Deny-List** tab is proposed.

Self-protection

For the "self-protection" level the **Allow-List** and **Deny-List DoS** tabs serve as a filter.

The **Allow-List** tab contains the list of IP addresses entered by the operator.

The **Deny-List DoS** tab contains the list of IP addresses identified by the SBC as coming from devices considered as attacking.

These IP addresses are contained in the security criteria defined for SIP DoS (flooding or Malicious call) attacks.

These addresses are automatically removed from the list after a configurable period (one hour by default).

The list of IP addresses on the Deny-List is configurable. When this limit is reached, the oldest entries are deleted.

Any request from a blacklisted IP address is not answered.

It is used to see, at an instant T, the non-trustworthy IP addresses preceded by the registration date and time.

Allow-List only

In this case, only the **Allow-List** tab is proposed, with the list of IP addresses entered by the operator.

It is used to manually define 100 trusted IP addresses .

DoS security parameters

The following three parameters concern DoS security.

- **Threshold**: 10 to 5000 (number of SIP requests authorised by window before incoming requests are blocked)
- **Window** (seconds): 2 to 10 (sampling period in seconds)
- **Period**: period after which the content of the DoS Deny-List is deleted; possible values are 30 seconds, 5 minutes, 30 minutes, 1 hour, 1 day, 1 week, indefinite.

DDoS security parameters

The following two values concern DDoS

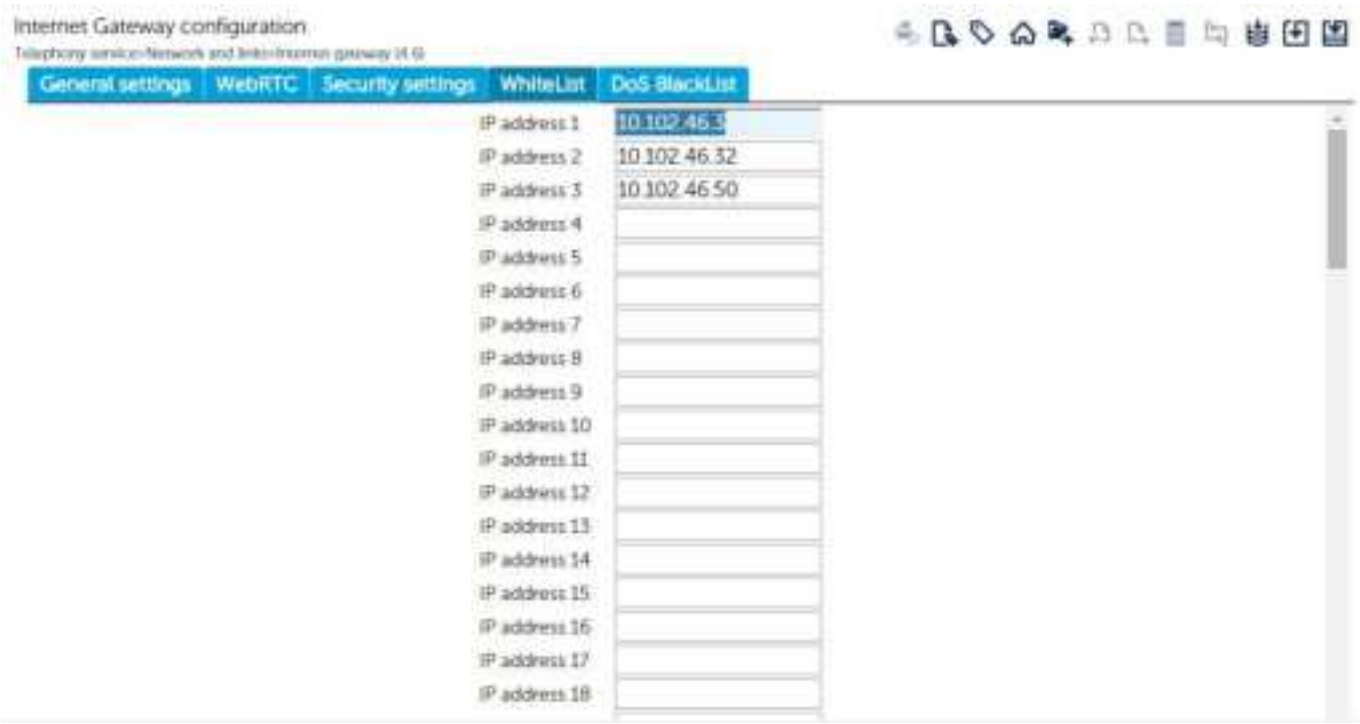
- **Threshold**: 10 to 5000 (number of SIP requests authorised by window before incoming requests are blocked)
- **Window** (seconds): 2 to 10 (sampling period in seconds)

Delete DoS Deny-List

After confirming the action, this option deletes all the DoS Deny-List inputs.

2.6.3 MANAGE ALLOW-LIST

Menu **NETWORK AND LINKS> Internet Gateway** – **Allow-List** tab



In this tab, each line is used to enter an IP address.

100 trusted IP addresses may be entered.

An error message is displayed when the field is validated.

2.6.4 MANAGE DOS DENY-LIST

Menu **NETWORK AND LINKS>Internet Gateway** – **Dos Deny-List** tab

Each line of the table displays a blacklisted address and is used to select the address to be deleted.

To delete an address, click on the hypertext link in the first column.

On this screen, the deletion is only effective if the confirmation button is pressed.

After the deletion, the DoS Deny-List is automatically opened.

On the deletion screen, the repeated command is possible, which is used to delete a series of addresses selected on the list of existing addresses from the one selected.

2.6.5 SECURITY LEVEL STATUS DURING A FIRST INSTALLATION OF R6.1

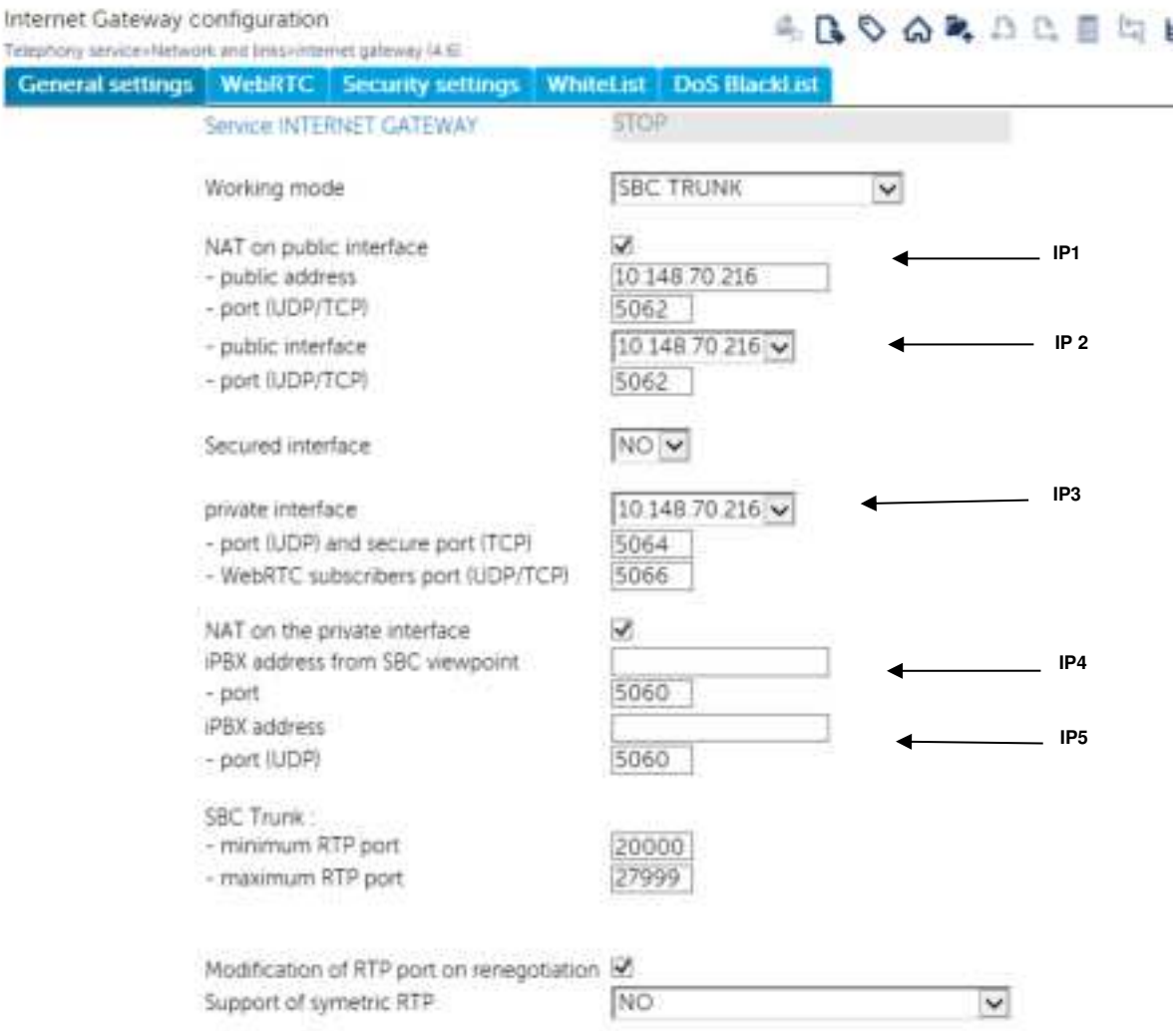
During a first installation, the security level is set to **self-protection.**

3 CONFIGURING THE SBC TRUNK

3.1 GENERAL PARAMETERS OF THE SBC SERVICE

Depending on the network architecture chosen, the menu **NETWORK AND LINKS>Internet Gateway – General parameters** tab is used to define the different addresses and ports associated with the SBC service:

- **IP1**: public IP address and port dedicated to the SBC service (used by the remote client to reach the SBC)
- **IP2**: private IP address and port of the SBC interface managing public traffic. This address must be chosen from the system interfaces.
- **IP3**: private IP address and port of the SBC interface managing private traffic. This address must be chosen from the system interfaces.
- **IP4**: private IP address and port dedicated to the SBC service used to reach the iPBX.
- **IP5**: IP address of the iPBX. By default, the address and port are those of the iPBX SIP service.



Note: The INTERNET GATEWAY Service line indicates the status of the SBC service. To modify it, click the hypertext link which redirects to the services configuration menu.

The box must be ticked when the NAT is implemented on the public network side.

- Enter the IP1 and IP2 addresses (respectively the SBC public address and interface).

Note: On the company's Firewall router, the static NAT must be implemented between IP1 and IP2.

If there is no NAT on the public side (the SBC has an interface with a public IP address):

- Enter **IP2** only.

IP1 is then automatically entered with the same value as **IP2**.

NAT on the private interface

The box must be activated when the NAT is performed on the private network side.

- Enter the **IP3** address and **IP4** address (private interface and address respectively).

If there is no NAT on the private side:

- Enter **IP3** only.

IP4 is then automatically entered with the same value as **IP3**.

Note that **IP1** and **IP4** can receive all the possible IP addresses. On the other hand, **IP2** and IP3 are restricted only to the IP addresses of the machine on which the MMC is executed.

The fifth address (**IP5**) is the PBX address, with its port (signalling part).

The RTP configuration includes the RTP port variation range (example 20,000 to 28,000) and the choice of RTP port change on an SIP renegotiation (audio/video flow part). The static NAT must be implemented on the router/firewall if IP2 does not have any public IP address.

Entering an incorrect IP address displays a "syntax error" message. The IP addresses 0.0.0.0 and 255.255.255.255 are not authorised.

Entering an incorrect RTP port displays the message "outside base stations", indicating the possible variation range. At least 4 ports are required for a radio communication (1 public RTP, 1 public RTCP, 1 private RTP and 1 private RTCP) and 8 in video.

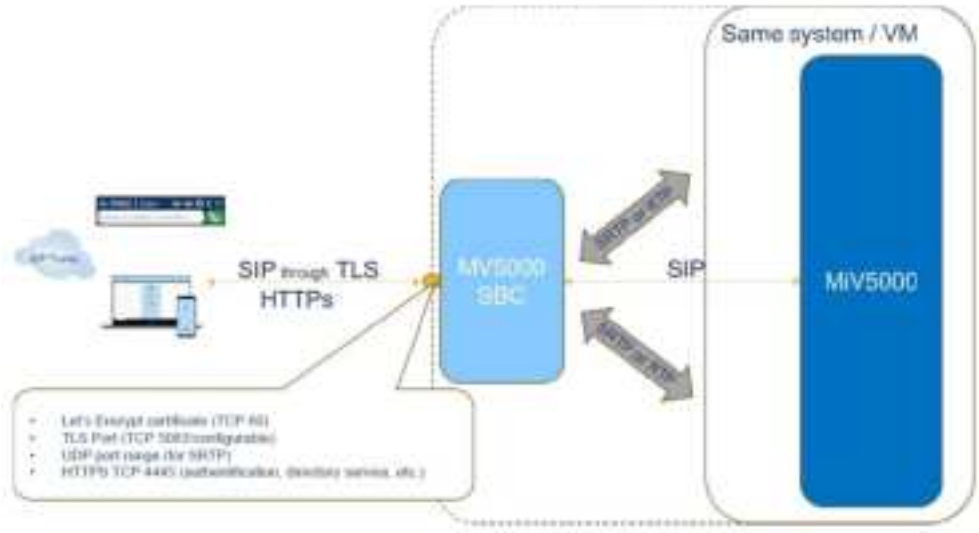
4 CONFIGURING SUBSCRIBERS IN OTT MODE

4.1 MITEL DIALER OTT

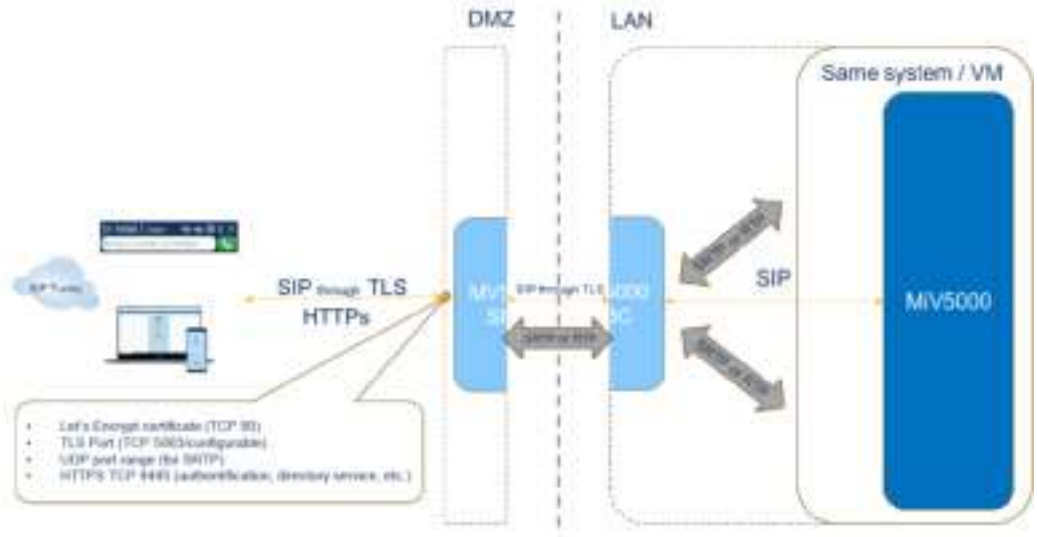
4.1.1 PRESENTATION

There is two ways of using the Mitel Dialer OTT:

- Standard configuration: The Mitel Dialer works with one MiVoice 5000 SBC in DMZ, whether the PBXis on the same machine or on different machines.



- Daisy Chain configuration: The Mitel Dialer works with 2 MiVoice 5000 SBC. The first one is in DMZ, the second one is in LAN



For more information about the possible configurations with the SBC, refer to the paragraph **2.3 – SBC Service architectures**.

The configuration contains 3 main steps:

- Configuring the SBC in the MiVoice 5000 Server (R8.2 SP2 minimum)
- Configuring the MiVoice 5000 Server (R8.2 SP2 minimum)
- Deploying the Mitel Dialer (R4.2 minimum).

4.1.2 PREREQUISITES

To configure the Mitel Dialer OTT, prepare the following elements:

- A ciphering license for the SBC,
- A user license with the Dialer option for the MiVoice 5000,

Note: Informations about the licence are available in the menu Telephony service>System>Info>Licenses.

- An imported (PKCS#12 or PEM) or a Let's Encrypt certificate to attribute to the service Internet Gateway,
- 1 DMZ IP address for the local address of the SBC,
- 1 public IP address for the SBC of the MiVoice 5000,
- 1 external FQDN resolved on the public IP address for the SBC,
  - If using the hybrid mode, this FQDN must be internally resolved on the Call Server.
- Open ports in the internal firewall.

  Refer to the following sections:
  - **4.1.3.2.1 – In a configuration standard SBC** for the ports to open in a standard configuration
  - **4.1.3.2.2 – In a Daisy Chain configuration** for the ports to open in a Daisy Chain configuration.

WARNING: Using MTLS trunks blocks the use of the OTT mode. To use the Mitel Dialer OTT and the OTT mode, disable the MTLS option

4.1.3 CONFIGURING THE SBC OF THE MIVOICE 5000

4.1.3.1 CONFIGURING THE CERTIFICATE MANAGEMENT MENU

Using the SBC requires a certificate attribution to the service Internet Gateway. It can either be an imported (PKCS#12 or PEM) or a Let's Encrypt certificate.

Menu **Telephony service>System>Security>Certificates management**, **Servers certificates assignment** tab

- In the **available certificates** dropdown menu, select the certificate to assign to the gateway.

  A table with the certificate information and a list of checkboxes appear.
- Check the Internet Gateway box.
- Click the **Validation** button to save the modifications.

4.1.3.2 CONFIGURING THE INTERNET GATEWAY MENU

4.1.3.2.1 *In a configuration with standard SBC*

Opening ports in the firewall

Configuring the Mitel Dialer OTT requires to open several ports in the internal firewall to work. Here are the ports to open in a standard SBC configuration:

- Ports from internet to the SBC:
  - TCP 4445 for the Web services for the Mitel Dialer OTT
  - TCP 5063 for the TLS SIP, the port for public protocols (configurable port).
  - UDP 20000-27999 for the voice (configurable range).
  - TCP 80 (optional) if using Let's Encrypt for certificate generation
- Port from the Call Server (LAN) to the SBC in DMZ
  - TCP 5065 for TLS SIP – port of private protocol (configurable)
- If the SBC of the MiVoice 5000 and the Call Server are on two different servers, open the following ports from DMZ to the destination IP of the Call Server only:
  - TCP 4445 for Web Services
  - TCP 5061 for the TLS SIP, the port to access the iPbx (configurable)
  - UDP 40000-41000 for the voice (configurable)
- For more information, refer to the document MiVoice 5000 Solution – List of TCP and UDP Ports.

In the MiVoice 5000 SBC

Menu **Telephony service>Network and links>Internet gateway**

- Verify that the **Secured interface** box is checked.
- If the **Both ways (MTLS)**option is visible, verify that the **Both ways (MTLS)** box is unchecked.
- Check the OTT terminals allowed box.

  A new field appears.
  - In the **FQDN public SBC** field, enter the FQDN resolved on the public IP address for the SBC.
- In the **Public protocols** dropdown menu, select **TLS**.

- Check the NAT on public interface box.

  New fields appear.

  - In the **public address** field, enter the public IP address for the Mitel Dialer OTT.
  - Verify that the **public interface** field is on the right IP address, according to the configuration.
  - In the **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5063.
- In the **Private protocols** dropdown menu, select **TLS**.
- In the **iPBX address or FQDN** field, enter the IP address of the Call Server.
- Configure the **minimum RTP port** (default: 20000) and **maximum RTP port** (default: 27999) fields according to the system configuration.

Menu **Telephony service>System>Configuration>Services**

- Check that the Service **INTERNET GATEWAY** parameter is on **START**.

4.1.3.2.2 *In a Daisy Chain configuration*

Opening ports in the firewall

Configuring the Mitel Dialer OTT requires to open several ports in the internal firewall to work. Here are the ports to open in a Daisy Chain configuration:

- Ports to open from internet to the SBC in DMZ:
  - Port TCP 4445 for the Web services for the Mitel Dialer OTT
  - Port TCP 5063 for the TLS SIP configuration (configurable port).
  - UDP 20000-27999 for the voice (configurable range).
  - TCP 80 (optional) if using Let's Encrypt for certificate generation
- Port to open from DMZ to LAN for the destination IP of the SBC LAN only:
  - TCP 4445 for Web Services
  - TCP 5063 for the TLS SIP, the port to access the LAN element (configurable)
  - UDP 20000-27999 for the voice (configurable)
- Port to open from the SBC in LAN to the SBC in WAN (DMZ):
  - TCP 5065 for TLS SIP – port of private protocol in SBC WAN (configurable)

For more information, refer to the document **MiVoice 5000 Solution – List of TCP and UDP Ports**.

In the MiVoice 5000 SBC in WAN mode

- In the **Mode** dropdown menu, select **Chained – WAN Element**.
- Verify that the **Secured interface** box is checked.
- Verify that the **Both ways (MTLS)** box is unchecked.
- Check the OTT terminals allowed box.

  A new field appears.
  - In the **FQDN public SBC** field, enter the public FQDN of the SBC.
- In the **Public protocols** dropdown menu, select **TLS**.

  Depending on the configuration of the MiVoice 5000, it is also possible to select **TLS + UDP/TCP**.
- Verify that the **public interface** field is on the right IP address, according to the configuration.
- Under the **Private protocols** parameter:
  - In the **LAN element address or FQDN** field, enter the address of the Call Server.
  - In the **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5063.
- Configure the **minimum RTP port** (default: 20000) and **maximum RTP port** (default: 27999) fields according to the system configuration.

In the MiVoice 5000 SBC in LAN mode

- In the **Mode** dropdown menu, select **Chained – LAN Element**.
- Verify that the **Secured interface** box is checked.

- According to the target configuration, it is possible to check the **Both ways (MTLS)** box.
- In the **Public protocols** dropdown menu, select **TLS**.

  Depending on the configuration of the MiVoice 5000, it is also possible to select **TLS + UDP/TCP**.
- Under the **Public protocols** parameter:
  - In the **WAN element address or FQDN** field, enter the address of the WAN SBC.
  - Verify that the **public interface** field is on the right IP address, according to the configuration.
  - In the second **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5063.
- Under the NAT on private protocols parameter:
  - In the **iPBX address or FQDN** field, enter the address of the LAN SBC.
  - In the **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5061.
- Configure the **minimum RTP port** (default: 20000) and **maximum RTP port** (default: 27999) fields according to the system configuration.

4.1.4 CONFIGURING THE MIVOICE 5000 SERVER

4.1.4.1 CHECKING THE VOICE CIPHERING AND GENERATING THE HASH

Menu **Telephony service>Network and links>Quality of service>Ciphering and IP settings**

- Verify that the **voice cyphering** box is checked.
- Verify if a hash already exists, via the **Files upload path** field.

  If the MiVoice 5000 already has a hash, go to section **2.4.3 – Activating the OpenID Connect SSO.**

WARNING: Generating a new hash in this case will impact all the deployed RemoteWorker devices.

If the MiVoice 5000 has no hash:

- In the **Hash generation** dropdown menu, select **OUI**.
- A popup appears to warn you on the risk of regenerating the hash. Click the **OK** button of the popup to close the popup.
- Click the **Confirmation** button to generate the new hash.

  A new field appears with the generated hash.

4.1.4.2 CHECKING THE OTT DETAILS OF THE MITEL DIALER

Menu **Telephony service>Subscribers>Terminals and applications>Dialer**

- Check the **OTT details** box to display the information dedicated to the Mitel Dialer OTT.
- Verify that the port in the **SIP/TLS port** field is the one dedicated to the TLS SIP of the SBC.

WARNING: If the SIP/TLS port changes after the procedure, modify the port in the menu Telephony service>Network and links>Internet gateway. The MiVoice 5000 automatically retrieves the port to assign it to the SIP/TLS port field of this menu.

- The Ciphered hash displays the hash dedicated tp the Mitel Dialer OTT. This field is linked to the hash in the menu **Telephony service>Network and links>Quality of service>Ciphering and IP settings.**

  If this field isn't displayed, verify that the MiVoice 5000 properly generated a hash in the menu **Telephony service>Network and links>Quality of service>Ciphering and IP settings**. Refer to the next section **2.4.2 – Checking the voice ciphering and generating the hash**.

4.1.4.3 ACTIVATING THE OPENID CONNECT SSO

The SSO OpenID Connect must be active for users. This is the authentication method that the Mitel Dialer uses.

To activate and configure the SSO OpenID Connect, go to the menu **Telephony service>Subscribers>Rights>General settings**, **SSO tab**.

Note: If the SSO via Open ID Connect is already configured in the MiVoice 5000 Server, the administrator must:

- **configure a new redirecting link on the existing provider application in the format https://[SBC FQDN]:4445/sso-oidc.**
- **Verify if each subscriber using the Mitel Dialer OTT has an email address in their internal record, so that the subscribers can log in.**

For more information on the fields to fill, refer to the document **MiVoice 5000 Server – Operating Manual**, section **3.9.1.1 –SSO tab**.

4.1.5 DEPLOYING THE MITEL DIALER

WARNING: Mitel Dialer OTT is compatible with Mitel Dialer R4.2 or later versions.

The deploying methods of the Mitel Dialer are available in the document **Mitel Dialer R4.2 – Installation and User Guide**.

4.1.6 ACCESSING THE USER PORTAL OF THE MITEL DIALER OTT

After configuring the OTT mode through the SBC of the MiVoice 5000, the User Portal is also accessible in OTT mode.

To access the User Portal, enter the link **https://[SBC FQDN]:4445/userportal/**, where **SBC FQDN** is the FQDN resolved on the public IP address of the SBC.

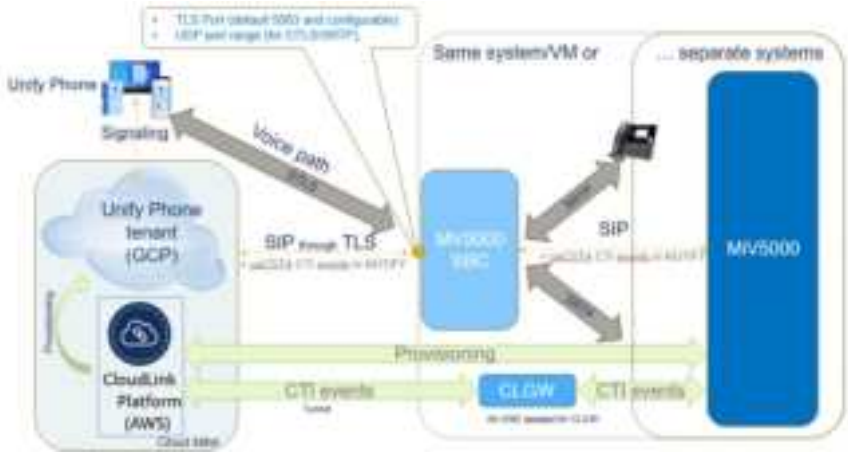
4.2 UNIFY PHONE

4.2.1 PRESENTATION OF UNIFY PHONE

Unify Phone is a app available on Android, IOS and PC through browser.

Unify Phone uses several Mitel services:

- CloudLink for the provisioning,
- The CloudLink Gateway for the CTI events,
- The MiVoice 5000 and the SBC of the MiVoice 5000 for the voices.



A standard configuration is recommanded for Unify Phone. The Daisy Chain configuration is possible. For more information about the possible configurations with the SBC, refer to the paragraph **2.3 – SBC Service architectures**.

The configuration contains 3 main steps:

- Configuring the SBC in the MiVoice 5000 Server (R8.2 SP3 minimum)
- Deploying and configuring CloudLink and the CloudLink Gateway
- Configuring the MiVoice 5000 Server (R8.2 SP3 minimum)

4.2.2 PREREQUISITES

To configure the Mitel Dialer OTT, prepare the following elements:

- A ciphering license for the SBC,
- A user license for Unify Phone,

Note: Informations about the licence are available in the menu Telephony service>System>Info>Licenses.

- 1 public static IP address,
- Deploying CloudLink and the CloudLink Gaeway. For more information about the installation and configuration of the CloudLink and CLoudLink Gateway, refer to the document **ClouLink – Deployment Guide with MiVoice 5000**.
- Open ports in the internal firewall.

  Refer to the following sections:

  - **4.2.3.2.1 – In a configuration with standard SBC** for the ports to open in a standard configuration
  - **4.2.3.2.2 – In a Daisy Chain configuration** for the ports to open in a Daisy Chain configuration.

The following element is optional, but recommended:

- 1 FQDN externally resolved on the public IP address. The FQDN is associated to a certificate given by a a public authority.

WARNING: Using MTLS trunks blocks the use of the OTT mode. To use Unify Phone and the OTT mode, disable the MTLS option.

If a MiVoice 5000 user is connected with both MiCollab and Unify Phone, the Microsoft Teams presence synchronization can't work for both MiCollab and Unify Phone

4.2.3 CONFIGURING THE SBC OF THE MIVOICE 5000

4.2.3.1 CONFIGURING THE CERTIFICATE FOR THE GATEWAY

Using the SBC requires a certificate attribution to the service Internet Gateway

In Unify Phone's case, if the Internet Gateway has no affected certificate, the MiVoice 5000 affects to the Internet Gateway a default certificate named defaultGW. The installer can also replace the default certificate with a Trusted certificate or a Lets' Encrypt certificate.

The affected certificate is displayed in the menu **Telephony service>System>Security>Certificates management**, **Servers certificates assignment** tab

4.2.3.2 CONFIGURING THE GATEWAY

4.2.3.2.1 *In a configuration with standard SBC*

Opening ports in the firewall

Configuring the Mitel Dialer OTT requires to open several ports in the internal firewall to work. Here are the ports to open in a standard configuration:

- Ports from internet to the SBC:
  - TCP 5063 for the TLS SIP, the port for public protocols (configurable port).
  - UDP 20000-27999 for the voice (configurable range).
  - TCP 80 (optional) if using Let's Encrypt for certificate generation
- Port from the Call Server (LAN) to the SBC in DMZ
  - TCP 5065 for TLS SIP – port of private protocol (configurable)
- If the SBC of the MiVoice 5000 and the Call Server are on two different servers, open the following ports from DMZ to the destination IP of the Call Server only:
  - TCP 5061 for the TLS SIP, the port to access the iPbx (configurable)
  - UDP 40000-41000 for the voice (configurable)
  - TCP 4445 (optional) for Web Services
- For more information, refer to the document MiVoice 5000 Solution – List of TCP and UDP Ports.

In the MiVoice 5000 SBC

Menu **Telephony service>Network and links>Internet gateway**

- Verify that the **Secured interface** box is checked.
- If using the MTLS options, verify that the **Both ways (MTLS)** box is unchecked.
- Check the OTT terminals allowed box.

A new field appears.

- In the **FQDN public SBC** field, enter the FQDN resolved on the public IP address for the SBC.

- In the **Public protocols** dropdown menu, select **TLS**.
- Check the NAT on public interface box.

  New fields appear.

  - In the **public address** field, enter the public IP address for the Mitel Dialer OTT.
  - Verify that the **public interface** field is on the right IP address, according to the configuration.
  - In the **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5063.
- In the **Private protocols** dropdown menu, select **TLS**.
- In the **iPBX address or FQDN** field, enter the IP address of the Call Server.
- Configure the **minimum RTP port** (default: 20000) and **maximum RTP port** (default: 27999) fields according to the system configuration.

Menu **Telephony service>System>Configuration>Services**

- Check that the Service **INTERNET GATEWAY** parameter is on **START**.

4.2.3.2.2 *In a Daisy Chain configuration*

Opening ports in the firewall

Configuring the Mitel Dialer OTT requires to open several ports in the internal firewall to work. Here are the ports to open in a Daisy Chain configuration:

- Ports to open from internet to the SBC in DMZ:
  - Port TCP 5063 for the TLS SIP configuration (configurable port).
  - UDP 20000-27999 for the voice (configurable range).
  - TCP 80 (optional) if using Let's Encrypt for certificate generation
- Port to open from DMZ to LAN for the destination IP of the SBC LAN only:
  - TCP 5063 for the TLS SIP, the port to access the LAN element (configurable)
  - UDP 20000-27999 for the voice (configurable)
  - TCP 4445 (optional) for Web Services
- Port to open from the SBC in LAN to the SBC in WAN (DMZ):
  - TCP 5065 for TLS SIP – port of private protocol in SBC WAN (configurable)

For more information, refer to the document **MiVoice 5000 Solution – List of TCP and UDP Ports**.

In the MiVoice 5000 SBC in WAN mode

- In the **Mode** dropdown menu, select **Chained – WAN Element**.
- Verify that the **Secured interface** box is checked.
- Verify that the **Both ways (MTLS)** box is unchecked.
- Check the OTT terminals allowed box.

  A new field appears.

  - In the **FQDN public SBC** field, enter the public FQDN of the SBC.

- In the **Public protocols** dropdown menu, select **TLS**.

  Depending on the configuration of the MiVoice 5000, it is also possible to select **TLS + UDP/TCP**.
- Verify that the **public interface** field is on the right IP address, according to the configuration.
- Under the **Private protocols** parameter:
  - In the **LAN element address or FQDN** field, enter the address of the Call Server.
  - In the **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5063.
- Configure the **minimum RTP port** (default: 20000) and **maximum RTP port** (default: 27999) fields according to the system configuration.

In the MiVoice 5000 SBC in LAN mode

- In the **Mode** dropdown menu, select **Chained – LAN Element**.
- Verify that the **Secured interface** box is checked.
- According to the target configuration, it is possible to check the **Both ways (MTLS)** box.
- In the **Public protocols** dropdown menu, select **TLS**.

  Depending on the configuration of the MiVoice 5000, it is also possible to select **TLS + UDP/TCP**.
- Under the **Public protocols** parameter:
  - In the **WAN element address or FQDN** field, enter the address of the WAN SBC.
  - Verify that the **public interface** field is on the right IP address, according to the configuration.
  - In the second **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5063.
- Under the NAT on private protocols parameter:
  - In the **iPBX address or FQDN** field, enter the address of the LAN SBC.
  - In the **secured port (TLS)** fields, enter the port dedicated to the TLS. The default port is 5061.
- Configure the **minimum RTP port** (default: 20000) and **maximum RTP port** (default: 27999) fields according to the system configuration.

4.2.4 CONFIGURING CLOUDLINK AND THE CLOUDLINK GATEWAY

4.2.4.1 PREREQUISITES

Using Unify Phone requires a CloudLink gateway.

For this, the installer must:

- Deploy CloudLink with the MiVoice 5000,
- Deploy a CloudLink Gateway,
- Configure Unify Phone on CloudLink.

This paragraph focuses on the last step.

For more information about deploying CloudLink and the CloudLink Gateway, refer to the document **CloudLink – Deployment Guide with MiVoice 5000**.

4.2.4.2 PROCEDURE

After deploying CloudLink and the CloudLink Gateway:

- Login in HTTP to the CloudLink Gateway portal through the IP address of the CloudLink Gateway,
- On the left, click the **Integration & Apps** menu.

Note: This interface is also available in the Account menu, under Integrations.

- Click the **+ Add new** button.

A window pops up with the list of the available integrations.

- In the **Mitel** tab, look for the **Unify Phone** integration anc click the according **Add** button.
- Click the **Done** button to close the window.
- Click the cog icon on the **Unify Phone** line to configure Unify Phone.

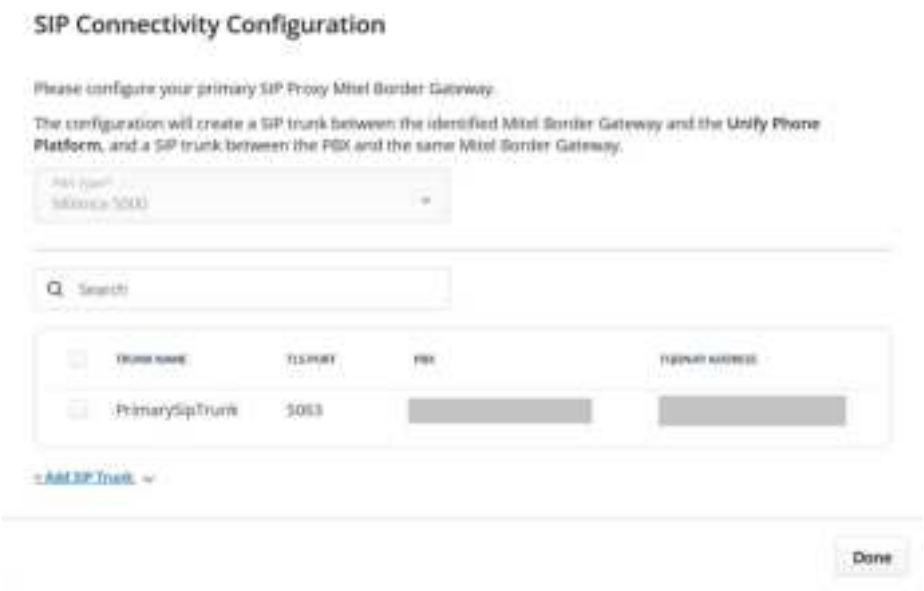
A new window opens to configure a tenant for. Unify Phone.

- Enter a name and the details on a CloudLink instance for Unify Phone:

- Click the **Available features** hyperlink to display the **SIP Connectivity** setting.
- Click the cog icon on the **SIP Connectivity** line to configure SIP trunk dedicated to Unify Phone.

A Window opens to configure a SIP trunk for Unify Phone. CloudLink automatically detects available SIP trunks for Unify Phone.

- Select a SIP trunk for Unify Phone:



4.2.5 CONFIGURNG THE MIVOICE 5000 CALL SERVER

WARNING: Before configuring the MiVoice 5000 Call Server, launch a resynchronization between the PBX and CloudLink in the menu Telephony service>Subscribers>Terminals and applications>Applications>CloudLink > Connection, Connection tab.

The resynchronization ensures the display of the CloudLink and Unify Phoen settings in the MiVoice 5000.

4.2.5.1 ALLOWING UNIFY PHONE RIGHTS TO CLOUDLINK ROLES

The installer affects the Unify Phone functionalities to subscribers through the CloudLink roles. The role management is in the menu **Telephony service>Subscribers>Terminals and applications>Applications>CloudLink>Roles**.

For more information about configuring CloudLink users, refer to the document **CloudLink – Deployment Guide with MiVoice 5000**.

In the Settings tab:

- In the **By name** dropdown menu, select the role to configure.
- Check the **Unify Phone** box. This option appears only after configuring the CloudLink Gateway for Unify Phone.

Menu **Telephony service>Subscribers>Subscriptions>Characteristics, Characteristics tab**

- In the designated subscriber records, select the createtd or modified CoudLink role for Unify Phone in the **CloudLink role** dropdown menu.
- Verify that the **Do not disturb allowed** box is checked. For new subscribers, the **Do not disturb allowed** box is checked by default.

4.2.5.2 CHECKING THE VOICE CIPHERING

Menu **Telephony service>Network and links>Quality of service>Ciphering and IP settings**

- Verify that the **voice cyphering** box is checked.